UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/802,646	03/16/2004	Harlan Seymour	20423-08590	3936

34415 7590 03/07/2008

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
LEWIS, ALICIA M	

ART UNIT	PAPER NUMBER
2164	

NOTIFICATION DATE	DELIVERY MODE
03/07/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com
bhoffman@fenwick.com
aprice@fenwick.com

Office Action Summary	Application No.	Applicant(s)	
	10/802,646	SEYMOUR ET AL.	
	Examiner	Art Unit	
	Alicia M. Lewis	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-11,14,15,17-20 and 23-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-11,14,15,17-20 and 23-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/16/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is responsive to the Request for Continued Examination (RCE) filed November 9, 2007. Claims 1, 5, 6, 14 and 15 have been amended, claims 12-13 and 21-22 have been canceled, and claims 23-26 have been added. Therefore, claims 1-6, 8-11, 14, 15, 17-20 and 23-26 are pending in this application.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-3, 5, 8, 9, 11, 14, 17, 18, 20 and 23-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mattsson (US Patent Application Publication 2003/0101355 A1) in view of Ludwig et al. (US Patent Application Publication 2003/0167229 A1).

With respect to claim 1, Mattson teaches an apparatus for empirically adjusting access to a database, said apparatus comprising:

coupled to the database, a database discovery module configured to determine database structure and authorized accesses to the database (paragraphs 32 and 34-36) until a preselected quantity of actual accesses have been observed (paragraphs 33 and

50) (*A preselected quantity can be any number of accesses, including just one access. In fact, the preselected quantity may be the number of accesses observed in a defined time period, as taught in paragraph 50 of Mattson*);

coupled to the database, a command monitoring module configured to monitor actual accesses to the database (paragraphs 33 and 50); and

coupled to the database discovery module and to the command monitoring module, an analysis module configured to compare actual accesses with authorized accesses and configured to adjust authorized accesses taking into account results of the comparing by changing settings within a database access control module (paragraphs 37-39, 42-46 and 52).

Mattson does not teach denying future database access to operations by certain users on database tables and columns that were previously authorized but not observed by the command monitoring module.

Ludwig teaches a modular business transactions platform (see abstract), in which he teaches denying future database access to operations by certain users on database tables and columns that were previously authorized but not observed by the command monitoring module (paragraph 51).

It would have been obvious to a person having ordinary skill in that art at the time the invention was made to have modified Mattson by the teaching of Ludwig because denying future database access to operations by certain users on database tables and columns that were previously authorized but not observed by the command monitoring module would enable Mattson's intrusion detection system to be used in processing

financial transactions and would provide more security measures to prevent intrusion, thus providing more functionality (Ludwig, paragraph 51).

With respect to claim 2, Mattson as modified teaches the apparatus of claim 1 further comprising, coupled to the database discovery module and to the analysis module, a storage area configured to accumulate data generated by the command monitoring module (Mattson, paragraph 33).

With respect to claim 3, Mattson as modified teaches the apparatus of claim 1 wherein the command monitoring module is a sniffer (Mattson, paragraph 5).

With respect to claims 5 and 14, Mattson as modified teaches:

discovering authorized accesses to the database (Mattson, paragraphs 32 and 34-36);

observing actual accesses to the database until a preselected quantity of actual accesses have been observed (Mattson, paragraphs 33 and 50) (*A preselected quantity can be any number of accesses, including just one access. In fact, the preselected quantity may be the number of accesses observed in a defined time period, as taught in paragraph 50 of Mattson)*;

comparing actual accesses with authorized accesses (Mattson, paragraphs 37 and 42); and

adjusting authorized database accesses taking into account results of the comparing step by changing settings within a database access control module of a computer-implemented database server to deny future database access to operations by certain users on database tables and columns that were previously authorized but were not observed during the observing step (Mattson, paragraphs 37-39, 42-46 and 52; Ludwig, paragraph 51).

With respect to claims 8 and 17, Mattson as modified teaches wherein the discovering step uncovers any:

tables of the database (Mattson, paragraph 32);

columns of the database (Mattson, paragraph 32);

authorized users of the database (Mattson, paragraph 34);

views of the database (Mattson, paragraph 32);

stored procedures of the database Mattson, (paragraph 53);

user-defined functions of the database (Mattson, paragraph 53); and

triggers of the database (Mattson, paragraph 53).

With respect to claims 9 and 18, Mattson as modified teaches wherein the adjusting step comprises at least one of:

suggesting revised database access control settings to a database administrator;

automatically hardening the database for all times of day (Mattson, paragraph 48);

automatically hardening the database selectively based on time of day;

alerting a database administrator (Mattson, paragraphs 43, 44 and 46); and

continuing to monitor accesses to the database after conclusion of the observing step.

With respect to claims 11 and 20, Mattson as modified teaches wherein the database is automatically hardened using database specific application programming interfaces (Mattson, paragraphs 46 and 48).

With respect to claim 23, Mattson as modified teaches wherein the preselected quantity of actual accesses is sufficiently large that all expected functionalities of applications accessing the database are exercised (Mattson, paragraphs 28-29, 33 and 50) *(The only expected functionalities of applications appears to be users using clients to access information in the database. Therefore, any preselected quantity of access to the database by clients, is large enough that the expected functionality is exercised).*

With respect to claim 24, Mattson as modified teaches storing data generated by the observing of actual accesses to the database in a storage area (Mattson, paragraph 33).

With respect to claim 25, Mattson as modified teaches generating a map of which tables and columns of the database were accessed during the observing (Mattson, paragraphs 32 and 33).

With respect to claim 26, Mattson as modified teaches:

monitoring actual accesses to the database during an extended period occurring after the preselected quantity of actual accessed have been observed (Mattson, paragraphs 35, 42 and 43) *(According to one embodiment, a preselected quantity may be the item access rate. When this is the case, an extended period may be considered any accesses that occur after the item access rate has been reached, as in paragraph 43);* and

generating an alert in real time regarding actual accesses that are observed during the extended period that were not observed within the preselected quantity of actual accesses (Mattson, paragraph 43) *(All accesses observed after the item access rate has been reached, are considered to be observed during the extended period, and not observed within the preselected quantity of accesses. When this is the case, as indicated in paragraph 43, an alert is generated.)*

3. Claim 4, 10 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mattsson (US Patent Application Publication 2003/0101355 A1) in view of Ludwig et al. (US Patent Application Publication 2003/0167229 A1), as applied to claims 1-3, 5,

8, 9, 11, 14, 17, 18, 20 and 23-26 above, and further in view of Low et al. ("DIDAFIT: Detecting Intrusions in Databases through Fingerprinting Transactions") ('Low').

With respect to claim 4, Mattson as modified teaches claim 1.

Mattson as modified does not teach wherein the database is a relational database accessed by a structured query language.

Low teaches a method for using fingerprints to detect illegitimate accesses to databases (see abstract) in which he teaches wherein the database is a relational database accessed by a structured query language (abstract).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Mattson by the teaching of Low because wherein the database is a relational database accessed by a structured query language would enable a fingerprinting process to be used to detect anomalous database accesses involving SQL statements (Low, column 1, page 122).

With respect to claims 10 and 19, Mattson as modified teaches wherein the database is automatically hardened using standard SQL commands (Low, abstract, page 126, column 1; Mattson, paragraphs 46 and 48).

4. Claims 6 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mattsson (US Patent Application Publication 2003/0101355 A1) in view of Ludwig et al. (US Patent Application Publication 2003/0167229 A1), as applied to claims 1-3, 5, 8, 9,

11, 14, 17, 18, 20 and 23-26 above, and further in view Vaitzblit et al. (US Patent Application Publication 2005/0097149 A1) (Vaitzblit').

With respect to claims 6 and 15, Mattson as modified teaches claims 5 and 14.

Mattson as modified does not teach further comprising the step of generating and storing at least one report based upon observing actual accesses to the database.

Vaitzblit teaches a data audit system (see abstract), in which he teaches further comprising the step of generating and storing at least one report based upon observing actual accesses to the database (paragraphs 11 and 48-51).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Mattson by the teaching of Vaitzblit because teach further comprising the step of generating at least one third party report based upon observing actual accesses to the database would enable an efficient data audit system that would help organizations address data privacy and security issues (Vaitzblit, paragraph 7), and to additionally detect anomalies (Vaitzblit, paragraph 19).

Response to Arguments

5. Applicant's arguments filed November 9, 2007 have been fully considered but they are not persuasive. Applicant argues that Mattson does not teach observing accessed until a preselected quantity of accesses have been observed. Examiner disagrees. A preselected quantity can be any number of accesses, including just one access. The claims do not recite a specific number of accesses, thus the number of

accesses observed may be considered the preselected number of accesses. In fact, the preselected quantity may be the number of accesses observed in a defined time period, as taught in paragraph 50 of Mattson. There is no step for actually selecting or determining a quantity of accesses to be observed, or no description of what the preselected quantity is. Thus the claim is given the broadest reasonable interpretation, and the preselected quantity may be considered the number of accesses observed in the defined time period.

6. Applicant further argues that the Examiner's interpretation is inconsistent with the specification and unreasonable because the specification distinguishes between observing accesses based on a preselected time period and accesses based on a preselected number. Section 2106 of the MPEP states, in part:

USPTO personnel are to give claims their broadest reasonable interpretation in light of the supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim should not be read into the claim. E-Pass Techs., Inc. v. 3Com Corp., 343 F.3d 1364, 1369, 67 USPQ2d 1947, 1950 (Fed. Cir. 2003) (claims must be interpreted "in view of the specification" without importing limitations from the specification into the claims unnecessarily). In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969). See also In re Zletz, 893 F.2d 319, 321-22, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989) ("During patent examination the pending claims must be interpreted as broadly as their terms reasonably allow.... The reason is simply that during patent prosecution when claims can be amended, ambiguities should be recognized, scope and breadth of language explored, and clarification imposed.... An essential purpose of patent examination is to fashion claims that are precise, clear, correct, and unambiguous. Only in this way can uncertainties of claim scope be removed, as much as possible, during the administrative process.").

7. Although claims are given their broadest reasonable interpretation in light of the supporting disclosure, limitations appearing in the specification but not recited in the claim should not be read into the claim. Therefore, just because the specification

provides two different ways to observe accesses, does not mean that those two different ways (or the differences between them) are read into the claims. According to the MPEP 2111 [R-5], "the PTO applies to verbiage of the proposed claims the broadest reasonable meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art, taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description contained in applicant's specification." The applicant's specification merely states that the observing step may be defined in terms of a time period, or alternatively in terms of a number of entries made to a storage area. There is nothing in the specification that limits that the number of entries from being a number of entries observed in a defined time period. Thus, one having ordinary skill in the art would agree that a number of accesses in a defined time period may be considered a preselected number of accesses.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Alicia M. Lewis whose telephone number is 571-272-5599. The examiner can normally be reached on Monday - Friday, 9 - 6:30, alternate Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Charles Rones can be reached on 571-272-4085. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Alicia Lewis
February 26, 2008

/Sam Rimell/
Primary Examiner, Art Unit 2164